IN THE CLAIMS

Please amend Claims 1-3, 8, 12-14, 16 and 18, and add claims 19-20 as follows:

1. (*Currently amended*) A method of authenticating a transaction, comprising ~~the steps of~~:

connecting a ~~card reader~~separate unit to a device having a keypad and display, the separate unit being secured and independently operating from the device;

initiating a transaction request using the device;

communicating the transaction request to a third party through the device; and

receiving a signal at the separate unit via the device to authenticate the transaction, wherein the separate unit is caused to request personalized data from a user associated with the device, the separate unit is not to encrypt the transaction but to authenticate the transaction between the device and the third party, the transaction can only be authenticated when the personalized data is authenticated in the separate unit.

2. (*Currently amended*) The method of claim 1, wherein the separate unit is a portable card reader unit is capable of reading a smartcard.

3. (*Currently amended*) The method of claim 1, wherein the separate unit is a portable card reader unit is capable of reading an optical card.

4. (*Original*) The method of claim 1, wherein the device is a personal digital assistant (PDA).

5. (*Original*) The method of claim 1, wherein the device is a telephone.

6. (*Original*) The method of claim 5, wherein the telephone is a cellular telephone.

7. (*Original*) The method of claim 1, wherein the signal used to authenticate the transaction is a high-contrast optical signal.

8. (*Currently amended*) The method of claim 1, wherein ~~the step of~~ said communicating the transaction request to ~~a device or~~ the third party involves ~~the~~ a use of a dual-tone audio signal.

9. (*Original*) The method of claim 8, wherein the signal is a dual-tone, multi-format (DTMF) signal.

10. (*Original*) The method of claim 8, wherein the signal is an audio frequency shift keying (AFSK) signal.

11. (*Original*) The method of claim 8, wherein the signal is a private line (PL) signal.

12. (*Currently amended*) The method of claim 1, wherein ~~the step of~~ said initiating a transaction request ~~at the card reader unit~~ includes ~~the~~ an entry of a personal identification number (PIN) through the keyboard of the device.

13. (*Currently amended*) The method of claim 12, wherein the separate ~~operation of the portable card reader~~ unit is terminated if a PIN entry is attempted more than a predetermined number of times.

14. (*Currently amended*) The method of claim 1, wherein~~:~~ the ~~card reader~~ separate unit further includes a biometric input; and ~~the step of~~ said initiating a transaction request ~~at the card reader unit~~ includes ~~the receipt of~~ receiving biometric data through the biometric input.

15. (*Original*) The method of claim 14, wherein the biometric input is a fingerprint.

16. (*Currently amended*) The method of claim 1, wherein one or both of the transaction request~~,~~ and the authentication signal~~, or both~~ are encrypted.

17. (*Original*) The method of claim 16, wherein the encryption is based on public-key cryptography.

18. (*Currently amended*) The method of claim 1, wherein~~:~~ the ~~card reader~~separate unit or device includes a memory; the transaction request and authentication signal constitute a session; and information regarding the session is stored in the memory.

19. (*Newly added*) The method of claim 1, wherein the separate unit is a headset.

20. (*Newly added*)The method of claim 19, wherein the headset includes capability of reading in confidential information from a user associated with the device.